Privacy Impact Assessment for the VA IT System called:

TriZetto Facets - ClaimsXM- E

VHA Office of Community Care

Date PIA submitted for review:

10-13-2020

System Contacts:

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Julie Drake</td>
<td><a href="mailto:Julie.Drake@va.gov">Julie.Drake@va.gov</a></td>
<td>303.331.7823</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Edgardo Rivera</td>
<td><a href="mailto:Edgardo.Rivera1@va.gov">Edgardo.Rivera1@va.gov</a></td>
<td>787.692.4583</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Christopher Brown</td>
<td><a href="mailto:Christopher.brown1@va.gov">Christopher.brown1@va.gov</a></td>
<td>202-270-1432</td>
</tr>
</tbody>
</table>
Abstract

The abstract provides the simplest explanation for “what does the system do?” and will be published online to accompany the PIA link.

TriZetto Facets -ClaimsXM, is a managed service system owned by the contractor Signature Choice LLC and it is hosted at Microsoft Azure Commercial Cloud- High. Signature Choice LLC subcontracts with Signature Performance Incorporated (Inc.), Principle Choice Solutions and Signature Performance Healthcare Administrative Services LLC. The service will receive community medical, dental and pharmacy claims, apply industry standard and VA specific business rules and policy to determine what, if any, payment is due to the provider. The system will ingest standard medical claim data, will maintain beneficiary eligibility and utilization data, and will display in or transport status and payment data to user-accessible portals and Veteran Affairs (VA) data systems.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes.
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

The TriZetto Facets - ClaimsXM- E is a contracted system for the Veteran Health Administration (VHA) Office of Community Care. The TriZetto Facets - ClaimsXM- E is a Signature Choice contractor owned system under a managed service contract to provide claims adjudication for VHA Office of Community Care. Expected number of individual records is in between 500,000- 600,000. The typical client are family members of eligible veterans receiving Veteran Affairs (VA) benefits. This system falls under VA\EPMO\Cloud. This system does not fall under the traditional regions (1-5).

The VHA Office of Community Care will transmit specified files via a Secure File Transfer Protocol (SFTP) server. The TriZetto Facets - ClaimsXM- E system will then retrieve the files from the SFTP server for processing within the system. Files will be returned to the VHA Office of Community Care by pushing files to the SFTP server and the VHA Office of Community Care pulling those files down. Additionally, TriZetto Facets - ClaimsXM- E will receive healthcare claims from VA’s Electronic Data Interchange (EDI) gateway for care provided to VA health care beneficiaries (Civilian Health and Medical Program of the Department of Veteran’s Affairs (CHAMPVA), Spina Bifida (SB), Children of Women Vietnam Veterans (CWVV)), TriZetto Facets - ClaimsXM- E will transfer payment instructions to VA’s financial management systems using file transfer. The components of the information system (servers) collecting/storing PII are Microsoft Azure Government Cloud Service – VM dynamic and AWS Microsoft Azure Government Cloud Service. The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of Health Insurance Portability and Accountability Act (HIPAA) and other Federal Regulatory information for the health care industry.

ClaimsXM employs Azure Site Recovery, which is a built-in feature in Azure. All the machines are set to replicate to another region. The ClaimsXM primary region is Arizona (AZ) and the secondary region is Texas (TX). The primary machines have disk replication in place. The ClaimsXM system is configured to automatically fall over to the alternate site. Alternate storage sites are established by way of Azure’s multiple geographic regions and across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. In the case of failure, automated processes move customer data traffic away from the affected area. The alternate storage sites are operated by Azure therefore, they have the same information security safeguards as that of the primary site.

The completion of this Privacy Impact Assessment (PIA) will not result in business process changes. The completion of this PIA will not result in technology changes. The development of this system will not affect the data collection, the System of Records Notice (SORN) listed will not require revision or modification.

This system employs cloud technology. TriZetto Facets -ClaimsXM, is a managed service, contracted with Signature Choice LLC and it is hosted at Microsoft Azure Government Cloud- High. FedRAMP agency authorization is currently in progress and sponsored by VA. FedRAMP authorization will follow issuance of the VA Authority to Operate (ATO).

The contract with Cloud Service Provider and contractor establishes who has ownership rights over data. Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the
resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct onsite inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

The magnitude of harm would be great as disclosures would affect healthcare transactions for individuals including both PHI and PII. The reputation of the cloud service provider (CSP) and/or the Department of Veteran Affairs may be affected.

Citation of Authority to operate:
38 U.S.C. § 1703 (Authorized care), Veterans Community Care Program
38 U.S.C. § 1728 (Unauthorized care), Reimbursement of certain medical expenses
38 U.S.C. § 1725 (Millennium Bill Act (Mill Bill)) Reimbursement for emergency treatment
38 U.S.C. § 1786 (Newborn care) Care for newborn children of women veterans receiving maternity care
38 U.S.C. § 7332 Confidentiality of certain medical records
38 C.F.R. § Chapter I Department of Veteran Affairs

System of Records Notices:
147VA10NF1, Enrollment and Eligibility Records-VA. Also, Privacy Notices provided in Program Guides and on the Program websites – July 14, 2016;
23VA10NB3, Non-VA Care (Fee) Records-VA – July 30, 2015;
24VA10A7, Patient Medical Records-VA – October 2, 2020;
38VA21, Veterans and Beneficiaries Identification Records Location Subsystem-VA (6-4-2001)
43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records-VA (4-6-2007)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA 3/3/2015
79VA10P2, Veterans Health Information Systems and Technology Architecture (VistA) –VA (10-31-2012)
88VA244, Accounts Receivable Records –VA; 147VA16, Enrollment and Eligibility Records-VA (4-6-1998)
Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy-Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system. This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Number (list below)

Date of Death (DOD), Member Identification Number, Patient Control Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Other Health Insurance Information, Other Health Insurance FMS Document ID, Paid Amounts, Member of the Public – Provider Tax Identification Number

PII Mapping of Components

TriZetto Facets - ClaimsXM- E consists of 3 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by TriZetto Facets - ClaimsXM- E and the reasons for the collection of the PII are in the table below.
### PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Azure Government Cloud Service – VM dynamic</td>
<td>Yes, the servers will process PII and PHI</td>
<td>Yes</td>
<td>Veterans or dependents – Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, FMS Document</td>
<td>Microsoft Azure Government Cloud Service – VM dynamic</td>
<td>Yes, the servers will process PII and PHI</td>
</tr>
<tr>
<td>Microsoft Azure Government Cloud Service</td>
<td>Yes, the database will store PII and PHI</td>
<td>YES</td>
<td>Veterans or dependents - Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed amounts, Other Health insurance Information, FMS Document ID, Paid Amounts.</td>
<td>Microsoft Azure Government Cloud Service</td>
<td>Yes, the database will store PII and PHI</td>
</tr>
<tr>
<td>TriZetto Facets Insights</td>
<td>Yes, the database will store PII and PHI</td>
<td>Yes</td>
<td>Veterans or dependents – Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification number, Patient Control Number, Medical Record Identification Number, Medical Record number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed amounts, Other Health Insurance Information, FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number</td>
<td>TriZetto Facets Insights</td>
<td>Yes, the database will store PII and PHI</td>
</tr>
</tbody>
</table>

1.2 What are the sources of the information in the system?
List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information. 
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The VHA Office of Community Care will transmit specified files via a Secure File Transfer Protocol (SFTP) server. The TriZetto Facets - ClaimsXM- E system will then retrieve the files from the SFTP server for processing within the system. Files will be returned to the VHA Office of Community Care by pushing files to the SFTP server and the VHA Office of Community Care pulling those files down. Additionally, TriZetto Facets - ClaimsXM- E will receive healthcare claims from VA’s Electronic Data Interchange (EDI) gateway for care provided to VA health care beneficiaries (CHAMPVA, Spina Bifida – SB, Children of Women Vietnam Veterans – CWVV). TriZetto Facets - ClaimsXM will transfer payment instructions to VA’s financial management systems using file transfer. Claims data is processed utilizing a VA aggregator, Change Health Care Clearing House.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The VHA Office of Community Care will transmit specified files via a Secure File Transfer Protocol (SFTP) server. The TriZetto Facets - ClaimsXM system will then retrieve the files from the SFTP server for processing within the system. Files will be returned to the VHA Office of Community Care by pushing files to the SFTP server and the VHA Office of Community Care pulling those files down. Additionally, TriZetto Facets - ClaimsXM will receive healthcare claims from VA’s Electronic Data Interchange (EDI) gateway for care provided to VA health care beneficiaries (CHAMPVA, Spina Bifida – SB, Children of Women Vietnam Veterans – CWVV). TriZetto Facets - ClaimsXM will transfer payment instructions to VA’s financial management systems using file transfer. From both Commercial aggregator and individuals
1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.

These data elements are used to positively identify the beneficiary: Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD) Address, Zip Code, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number

These data elements are used to process and associate claims to a beneficiary: Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number

1.5 How will the information be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Daily, due to claims lifecycle utilizing a VA aggregator, Change Health Care Clearing House. The VHA Office of Community Care will transmit specified files via a Secure File Transfer Protocol (SFTP) server. The TriZetto Facets - ClaimsXM- E system will then retrieve the files from the SFTP server for processing within the system. Files will be returned to the VHA Office of Community Care by pushing files to the SFTP server and the VHA Office of Community Care pulling those files down. Additionally, TriZetto Facets - ClaimsXM- E will receive healthcare claims from VA’s Electronic Data Interchange (EDI) gateway for care provided to VA health care beneficiaries (CHAMPVA, Spina Bifida – SB, Children of Women Vietnam Veterans – CWVV). TriZetto Facets - ClaimsXM will transfer payment instructions to VA’s financial management systems using file transfer. Claims data is processed utilizing a VA aggregator, Change Health Care Clearing House.
1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

This question is related to privacy control AP-1, Authority to Collect

38 U.S.C. § 1703 (Authorized care), Veterans Community Care Program
38 U.S.C. § 1728 (Unauthorized care), Reimbursement of certain medical expenses
38 U.S.C. § 1725 (Millennium Bill Act (Mill Bill)) Reimbursement for emergency treatment
38 U.S.C. § 1786 (Newborn care) Care for newborn children of women veterans receiving maternity care
38 U.S.C. § 7332 Confidentiality of certain medical records
38 C.F.R. § Chapter I Department of Veteran Affairs

System of Records Notices:
147VA10NF1, Enrollment and Eligibility Records-VA. Also, Privacy Notices provided in Program Guides and on the Program websites – July 14, 2016;
23VA10NB3, Non-VA Care (Fee) Records-VA – July 30, 2015;
24VA10A7, Patient Medical Records-VA – October 2, 2020;
38VA21, Veterans and Beneficiaries Identification Records Location Subsystem-VA (6-4-2001)
43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records-VA (4-6-2007)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA 3/3/2015
79VA10P2, Veterans Health Information Systems and Technology Architecture (VistA) –VA (10-31-2012)
88VA244, Accounts Receivable Records –VA; 147VA16, Enrollment and Eligibility Records-VA (4-6-1998)

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

**Principle of Purpose Specification:** Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

**Principle of Minimization:** Is the information directly relevant and necessary to accomplish the specific purposes of the program?

**Principle of Individual Participation:** Does the program, to the extent possible and practical, collect information directly from the individual?
**Principle of Data Quality and Integrity:** Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current? This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

**Privacy Risk:** There is a potential privacy risks that the data is inaccurate when transmitted to the TriZetto Facets-Claims XM-E system.

**Mitigation:** Data received by the VA is verified by the VA before transmission to the TriZetto Facets-Claims XM-E system. Data is encrypted during transit and at rest when received and maintained in the TriZetto Facets-Claims XM-E system.

**Section 2. Uses of the Information**

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program’s business purpose.

_Identify and list each use (both internal and external to VA) of the information collected or maintained._

This question is related to privacy control AP-2, Purpose Specification.

These data elements are used to positively identify the beneficiary: Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number.

These data elements are used to process and associate claims to a beneficiary: Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly
created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

TriZetto Facets Insights is used to analyze the number of claims processed for given periods of time. The tool used to analyze data is TriZetto Facets Insights.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e., denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Access to PII by Signature Choice’s associates will be based on a need to know to perform the Associate’s job function. Additionally, system access is based on Role Based Access Controls (RBAC). The RBAC model will ensure proper separation of duties in the system. Access to the system will be requested through the IT ticketing system where the Associate’s manager will need to provide approval for the system access. Once access has been approved the Associates profile will be developed based on the designated RBAC model for the Associates job function. Upon termination of employment the Associate’s access to the system is removed immediately. System access is reviewed quarterly and documented in the ticketing system.

Access to the TriZetto Facets - ClaimsXM system is being logged and monitored through a Security Information and Event Management (SIEM) solution managed and maintained by Signature Choice.
Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Date of Death (DOD), Member Identification Number, Patient Control Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Other Health Insurance Information, Other Health Insurance FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.

The contractor will follow the VHA Records Retention Schedule 10-1 @ https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf.

Sections 1260- Civilian Health and Medical Care Program and 4000- Financial Management and Reporting Records or 6000- Health Information Management Service (HIMS)

Also, procedures under the contract, Media Sanitization Policy (OIT-OIS SOP MP-6-Electronic Media Sanitization) and Records Management Policy (VHA Directive 6300 Records Management).

1260 Care in Community, Health and Medical Care Program, VA. Compensation, Pension and Vocational Rehabilitation, Records Control Schedule 10-1, 1180 1180 Office of General Counsel; VA Central Office (VACO) and Regional Offices; 1180.17. Veterans Benefits.
3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. This question is related to privacy control DM-2, Data Retention and Disposal.

Record Control Schedule (RCS) 10–1 item (http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf).

3.4 What are the procedures for the elimination of SPI?

*Explain how records are destroyed or eliminated at the end of the retention period.* Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

This question is related to privacy control DM-2, Data Retention and Disposal

Prior to termination or completion of this contract, Signature must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and VA Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and Media Sanitization Policy (OIT-OIS SOP MP-6-Electronic Media Sanitization), Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans’ Affairs VA Directive 6371, (April 8, 2014), [https://www.va.gov/vapubs](https://www.va.gov/vapubs)

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the *Department of Veterans’ Affairs Handbook 6500.1, Electronic Media Sanitization* (November 3, 2008), [https://www.va.gov/vapubs](https://www.va.gov/vapubs). When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.

Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

*Organizations often use PII for testing new applications or information systems prior to deployment.* Organizations also use PII for research purposes and for training. These uses of PII increase the
risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

No, the system does not allow for this and third-party service providers are not permitted to do so either. All testing data is deidentified prior to transference, use and testing.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

**Principle of Minimization:** Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

**Principle of Data Quality and Integrity:** Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

**Privacy Risk:** There is a risk that the information maintained by TriZetto Facets ClaimsXM could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

**Mitigation:** To mitigate the risk posed by information retention, TriZetto Facets ClaimsXM adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual’s information is carefully disposed of by the determined method as described in the records control schedule.

**Section 4. Internal Sharing/Receiving/Transmitting and Disclosure**

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.
4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information? This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Office of Information Technology Veterans Data Integration and Federation Enterprise Platform</td>
<td>The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.</td>
<td>Veterans or dependents - Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code</td>
<td>Secure File Transfer Protocol (SFTP)</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific data element types such as PHI/PHI that are shared/received with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>VA Enterprise Cloud Amazon (AWS) Payer Electronic Data Interchange (EDI) Transactions Application Suite (TAS)</td>
<td>The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.</td>
<td>Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number</td>
<td>SFTP</td>
</tr>
<tr>
<td>Veterans Health Administration Office Community Care Claims Processing</td>
<td>The information being shared is for the Claims Processing of Veteran Family</td>
<td>Veterans or dependents - Patient Name, Social Security Number SSN), Date of Birth (DOB), Date of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Controlumber, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number</td>
<td>SFTP</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific data element types such as PHI/PHI that are shared/received with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>and Eligibility (CP&amp;E)</td>
<td>Member Program claims. The data and information follows health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.</td>
<td>(SSN), Date of Birth (DOB), Date of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number</td>
<td>File Transfer Protocol with SSL Security</td>
</tr>
<tr>
<td>Financial Service Center (FSC)</td>
<td>The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.</td>
<td>Veterans or dependents - Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing</td>
<td></td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific data element types such as PHI/PHI that are shared/received with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>VA Enterprise Cloud Microsoft Azure Program Integrity Tool</td>
<td>The information being shared is for the Claims Processing of Veteran Family Member Program claims. The data and information follow health care industry standards for the exchange of HIPPA and other Federal Regulatory information for the health care industry.</td>
<td>Information (Claim Index), Billed Amounts, Other Health Insurance Information, FMS Document ID, Paid Amounts, Member of the Public – Provider Tax Identification Number. Veterans or dependents - Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number</td>
<td>SFTP</td>
</tr>
</tbody>
</table>
4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA programs or systems.

Mitigation: This is a cloud-based system where the CSP 3PAO already conducts penetration testing and defense in depth. Flaw remediation is centrally managed through four separate processes: -- The deployment of antivirus configurations to all system servers -- The use of configuration management to centrally manage the identification of all required Windows patches and to install them on appropriate servers -- The use of Ansible to centrally manage the identification of all required Linux patches and to install them on appropriate servers -- Monthly Nessus scanning informs system staff of required security vulnerabilities and fixes. System staff also conducts its own monthly Nessus scans to identify and interpret system vulnerabilities. Scanning results are reported, analyzed and recorded for remediation. The information system fails to a stopped state for database integrity and disk space problems, preserving existing data and audit records in failure. Systems are backed up continuously to an alternate site. In the event of a catastrophic failure, the system can be restored from alternate site or failed over to run at the alternate site. As stated within the Azure System Security Plan, Azure will prevent the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. Data confidentiality and integrity is ensured via administrative, technical and physical controls. Physical access to the servers is restricted to authorized personnel in a data center at a facility with 24-hour security. Network access to servers is managed through firewalls. Access via the network requires authentication for both the application and servers.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Note: This question is #7 in the Privacy Threshold Analysis.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.
For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission. This question is related to privacy control UL-2, Information Sharing with Third Parties.
<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Health Care Clearing House</td>
<td>Claims processing. Data Transmission through SFTP</td>
<td>Veterans or dependents - Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number</td>
<td>Contract, ISA/MOU, BAA</td>
<td>Business Partner Extranet (BPE)</td>
</tr>
<tr>
<td>Signature</td>
<td>Claims processing. Data</td>
<td>Veterans or dependents -</td>
<td>MOU/ISA BAA</td>
<td>Business Partner</td>
</tr>
<tr>
<td>Performance (sub-contractor)</td>
<td>Transmission through SFTP</td>
<td>Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, FMS Document ID, Paid Amounts, Member of the Public – Provider Tax Identification Number</td>
<td>Extranet (BPE) [Business Partner Extranet [BPE], firewall, and other connections] on and to a VA. Trusted Internet Connection (TIC) Gateway</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Globalscape (system)</td>
<td>Claims processing. Data Transmission through SFTP</td>
<td>Veterans or dependents - Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD), Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Information</td>
<td>ISA/MOU BAA</td>
<td>S2S VPN Tunnel [Trusted Internet Connection (TIC) Gateway.]</td>
</tr>
<tr>
<td>Pharmacy Benefits Manager</td>
<td>Claims processing, Data Transmission through SFTP</td>
<td>Veterans or dependents - Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information</td>
<td>MOU/ISA BAA</td>
<td>Business Partner Extranet (BPE)</td>
</tr>
<tr>
<td>Principle Choice Solutions (Subcontractor)</td>
<td>Claims processing. Data Transmission through SFTP</td>
<td>Veterans or dependents - Patient Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD) Address, Zip Code, Address, Zip Code, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers (Policy Number), Plan Name, CPT and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, FMS Document ID, Paid Amounts. Member of the Public – Provider Tax Identification Number</td>
<td>ISA/MOU BAA</td>
<td>Business Partner Extranet (BPE)</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

All data in encrypted while at rest and when transmitted electronically. Appropriate security controls are in place to guard against unauthorized access to the data.
5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

**Privacy Risk:** There is a risk that information may be shared with an unauthorized program, system, or individual.

**Mitigation:** All users with access to Trizetto Facets- Claim XM undergo Privacy and Security training (VA10176 or equivalent) and sign a Rules of Behavior. There are penalties for non-compliance with rules of behavior for VA users and contractual penalties for the vendor. Access is limited based on need to know.

Data confidentiality and integrity is ensured via a variety of administrative, technical and physical controls. Information is protected by FIPS 140-2 approved encryption at rest and in transit. Separation of duties controls are in place. Transactions are logged and audit logs are reviewed for events affecting privacy and security.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Notice is provided to beneficiaries are provided upon enrollment. A form of this notice is provided in the CHAMPVA Guide.

1. Privacy notices are provided at the point of service at the medical center or facility under Health Information Access and Accountability (HIPAA) where the beneficiary receive care, in accordance with VHA Handbook 1605.4, Notice of Privacy Practices.
2. Notice of privacy practices are available on the [https://www.va.gov/privacy/](https://www.va.gov/privacy/)

Each of the above notices includes information on how to report any use of information that is not in accordance with the collection.

Refer to Appendix A: Notice of Privacy Practices for a link to the notice of privacy practices provided at all VAMCs.

System of records notices that apply to the collection, use and disclosure of information within this data collection.

Link: [https://www.oprm.va.gov/docs/CurrentSORNList_4_29_20.pdf](https://www.oprm.va.gov/docs/CurrentSORNList_4_29_20.pdf)

147VA10NF1, Enrollment and Eligibility Records-VA. Also, Privacy Notices provided in Program Guides and on the Program websites – July 14, 2016;
23VA10NB3, Non-VA Care (Fee) Records-VA – July 30, 2015;
24VA10A7, Patient Medical Records-VA – October 2, 2020;
38VA21, Veterans and Beneficiaries Identification Records Location Subsystem-VA (6-4-2001)
43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records-VA (4-6-2007)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA 3/3/2015
79VA10P2, Veterans Health Information Systems and Technology Architecture (VistA) –VA (10-31-2012)
88VA244, Accounts Receivable Records –VA; 147VA16, Enrollment and Eligibility Records-VA (4-6-1998).

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

There is no alternative to receiving correct payment from the VA. Privacy Rights are afforded at the time of service. A person can refuse to provide personal information at that time but will not receive services. Revocation of Authorization. If you provide us a written authorization or permission to use or disclose your health information, you may revoke that permission, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information except to the extent that VHA has relied on your written authorization. Please understand that we are unable to take back any uses or disclosures we have already made based on your authorization. YOUR PRIVACY RIGHTS Right to
Request Restriction. You may request that we not use or disclose all or part of your health information to carry out treatment, payment or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person. Please be aware, we are not required to agree to such restriction, except in the case of a disclosure restricted under 45 C.F.R. § 164.522(a)(1)(vi). This provision applies only if the disclosure of your health information is to a health plan for the purpose of payment or health care operations and your health information pertains solely to a health care service or visit which you paid in full. However, VHA is not legally able to accept an out of pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services provided to you. To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you no longer make the restriction request valid or you revoke it.

IB 10-163, Notice of Privacy Practices, VA Poster 10-163 (large format, print-ready version), 10A7B - Health Information Governance

https://www.va.gov/vhapublications/publications.cfm?pub=8

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?

This question is related to privacy control IP-1, Consent

Individuals have a right to contact the VHA call center to gain access to their information.

See Appendix A: Notice of Privacy Practices for a link to the notice of privacy practices provided at all VAMCs, which includes the following:

Other Uses and Disclosures with Your Authorization. We may use or disclose your health information for any purpose based on a signed, written authorization you provide us. Your signed written authorization is always required to disclose your psychotherapy notes if they exist. If we were to use or disclose your health information for marketing purposes, we would require your signed written authorization. In all other cases, we will not use or make a disclosure of your health information without your signed, written authorization, unless the use or disclosure falls under one of the exceptions described in this Notice. When we receive your signed written authorization, we will review the authorization to determine if it is valid, and then disclose your health information as requested by you in the authorization. Revocation of Authorization. If you provide us a written authorization or permission to use or disclose your health information, you may revoke that permission, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information except to the extent that VHA has relied on your written authorization. Please understand that we are unable to take back any uses or disclosures we have already made based on your authorization.
6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following FIPPs below to assist in providing a response:

**Principle of Transparency:** Has sufficient notice been provided to the individual?

**Principle of Use Limitation:** Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

**Privacy Risk:** Sufficient notice has not been provided to the individual therefore the individuals are unaware that their information is being collected.

**Mitigation:** This system does not collect data directly. Privacy Rights are provided at the point of care and through program guides individuals are notified that their information is being collected and used. Individuals can decline to provide information, as a result services will be delayed. Data is encrypted at rest.

**Section 7. Access, Redress, and Correction**

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

**7.1 What are the procedures that allow individuals to gain access to their information?**

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).
If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Privacy notice provided at the point of service addressed redress, see appendix A. Any records generated by the system will be the responsibility of the VA to maintain, retain, and act upon any applicable Freedom of Information Act, Privacy Act, or HIPAA requests. Individuals can submit a request for information through the VHA Office of Community Care FOIA/Privacy Office vha.occ.po@va.gov or vha.occ.FOIA@va.gov.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

To correct data in VHA Systems the Beneficiary will call the VHA Call center at: 1-916-692-7450

Beneficiary Customer service telephone line: 1-800-733-8387

Right to Request Amendment of Health Information. You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

• File an appeal
• File a “Statement of Disagreement”
• Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Beneficiary will call the VHA Call center at: 1-916-692-7450
Beneficiary Customer service telephone line: 1-800-733-8387

Right to Request Receipt of Communications in a Confidential Manner. You have the right to request that we provide your health information to you by alternative means or at an alternative location. We will
accommodate reasonable requests, as determined by VA/VHA policy, from you to receive communications containing your health information:
• At a mailing address (e.g., confidential communications address) other than your permanent address
• In person, under certain circumstances.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Beneficiary will call the VHA Call center at: 1-916-692-7450

Beneficiary Customer service telephone line: 1-800-733-8387.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: If the VHA OCC employee enters the data incorrectly, and the veteran/beneficiary is not paid accurately.

Mitigation: The Veteran/Beneficiary or provider can contact the claims payment customer service support telephone line, Beneficiary: 1-800-733-8387 or they may contact the VHA OCC Privacy office vha.occ.po@va.gov.
Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Access to PII by Signature Performance Associates will be based on a need to know to perform the Associate’s job function. Additionally, system access is based on Role Based Access Controls (RBAC). The RBAC model will ensure proper separation of duties in the system. Access to the system will be requested through the IT ticketing system where the Associate’s manager will need to provide approval for the system access. Once access has been approved the Associates profile will be developed based on the designated RBAC model for the Associates job function.

There are no users from other agencies that have access to the TriZetto Facets - ClaimsXM system. Administrators, Domain Admins and Service Accounts, are privileged accounts, these functions are issued for use and management of applications, devices and systems and used to run services such as backups/restores. User accounts Identification are general user accounts and use data viewer/manipulation. Process identification rolls are application accounts, these include general user functions.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Signature Choice, a contractor of the VA, are required to sign non-disclosure agreements as part of their VA security clearance. Contractors will have access to the system to perform claim adjudication and
system administrative functions. The design and maintenance of the system is maintained and performed by Signature Choice. There are proper contracts in place with Signature Choice. The contract is reviewed by the contracting officer every five (5) years.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Privacy and Security Training
- Security awareness (cyber awareness) and HIPAA Security and Privacy Rule training is administered VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics Role-based Training
Includes, but is not limited to and based on the role of the user.
VA 1016925: Information Assurance for Software Developers IT Software Developers
VA 3193: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
VA 1357084: Information Security Role-Based Training for Data Managers
VA 64899: Information Security Role-Based Training for IT Project Managers
VA 3197: Information Security Role-Based Training for IT Specialists
VA 1357083: Information Security Role-Based Training for Network Administrators
VA 1357076: Information Security Role-Based Training for System Administrators
VA 3914020 Contingency Plan Role Based Training

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.

If No or In Process, provide your Initial Operating Capability (IOC) date.

The system categorization was determined to be moderate. This is in process. Initial Operating Capability date is 01/01/2021.
### Section 9. References

**Summary of Privacy Controls by Family**

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td><strong>Authority and Purpose</strong></td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td><strong>Accountability, Audit, and Risk Management</strong></td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td><strong>Data Quality and Integrity</strong></td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td><strong>Data Minimization and Retention</strong></td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td><strong>Individual Participation and Redress</strong></td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td><strong>Transparency</strong></td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td><strong>Use Limitation</strong></td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms). CHAMPVA Guide located at: https://www.va.gov/COMMUNITYCARE/docs/pubfiles/programguides/champva_guide.pdf


Department of Veterans Affairs Veterans Health Administration
NOTICE OF PRIVACY PRACTICES
Effective Date September 30, 2019

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED OR DISCLOSED AND HOW YOU CAN GET ACCESS TO YOUR INFORMATION. PLEASE REVIEW IT CAREFULLY

The Department of Veterans Affairs (VA), Veterans Health Administration (VHA) is required by law to maintain the privacy of your protected health information and to provide you with notice of its legal duties and privacy practices. VHA may use or disclose your health information without your permission for treatment, payment and health care operations, and when otherwise required or permitted by law. This Notice outlines the ways in which VHA may use and disclose your health information without your permission as required or permitted by law. For VHA to use or disclose your information for any other purposes, we are required to get your permission in the form of a signed, written authorization. VHA is required to maintain the privacy of your health information as outlined in this Notice and its privacy policies. Please read through this Notice carefully to understand your privacy rights and VHA’s obligations.

YOUR PRIVACY RIGHTS
Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314)801-0800. The Web site is http://www.archives.gov/veterans/military-service-records/medical-records.html.

Right to Request Amendment of Health Information. You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information or health records.

If your request for amendment is denied, you will be notified of this decision in writing and given information about your right to appeal the decision. In response, you may do any of the following:
• File an appeal.
• File a “Statement of Disagreement” which will be included in your health record
• Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

Right to Request Receipt of Communications in a Confidential Manner. You have the right to request that we provide your health information to you by alternative means or at an alternative location. We will accommodate reasonable requests, as determined by VA/VHA policy, from you to receive communications containing your health information:
• At a mailing address (e.g., confidential communications address) other than your permanent address.
• In person, under certain circumstances.

Right to Request Restriction. You may request that we not use or disclose all or part of your health information to carry out treatment, payment or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person.
Please be aware, that because VHA, and other health care organizations are “covered entities” under the law, VHA is not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1)(vi). This provision applies only if the disclosure of your health information is to a health plan for the purpose of payment or health care operations and your health information pertains solely to a health care service or visit which you paid out of pocket in full. However, VHA is not legally able to accept an out of pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services VA provided to you.

To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you revoke it unless the information covered by the restriction is needed to provide you with emergency treatment or the restriction is terminated by VHA upon notification to you.

NOTE: We are not able to honor requests to remove all or part of your health information from the electronic database of health information that is shared between VHA and DoD, or to restrict access to your health information by DoD providers with whom you have a treatment relationship.

Right to Receive an Accounting of Disclosures. You have the right to know and request a copy of what disclosures of your health information have been made to you and to other individuals outside of VHA. To exercise this right, you must submit a written request to the facility Privacy Officer at the VHA health care facility that provides your care.

Right to a Printed Copy of the Privacy Notice. You have the right to obtain an additional paper copy of this Notice from your VHA health care facility. You can obtain this Notice from the facility Privacy Officer at your local VHA health care facility. You may also obtain a copy of this Notice at the following website: http://www.va.gov/vhapublications.

Notification of a Breach of your Health Information. If a breach of any of your protected health information occurs, we will notify you and provide instruction for further actions you may take, if any.

Complaints. If you are concerned that your privacy rights have been violated, you may file a complaint with:

The Privacy Officer at your local VHA health care facility. Visit this Web site for VHA facilities and telephone numbers
http://www1.va.gov/directory/guide/home.asp?isflash=1 • VA via the Internet through “Contact the VA” at http://www.va.gov or by dialing 1-800-983-0936 or by writing the VHA Privacy Office (10A7) at 810 Vermont Avenue NW, Washington, DC 20420.
• The U.S. Department of Health and Human Services, Office for Civil Rights at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html
• Complaints do not have to be in writing, though it is recommended. An individual filing a complaint will not face retaliation by any VA/VHA organization or VA/VHA employee.

When We May Use or Disclose Your Health Information without Your Authorization

Treatment. We may use and disclose your health information without your authorization for treatment or to provide health care services. This includes using and disclosing your information for:

• Emergency and routine health care or services, including but not limited to labs and x-rays; clinic visits; inpatient admissions
• Contacting you to provide appointment reminders or information about treatment alternatives
• Seeking placement in community living centers or skilled nursing homes
• Providing or obtaining home-based services or hospice services
• Filling and submitting prescriptions for medications, supplies, and equipment
• Coordination of care, including care from non-VHA providers,
• Communicating with non-VHA providers regarding your care through health information exchanges
• Coordination of care with DoD, including electronic information exchange
Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

JULIE C. DRAKE
969177
Digitally signed by JULIE C. DRAKE 969177
Date: 2020.10.28 14:36:29 -06'00'

PO, Julie Drake

EDGARDO RIVERA-URRUTIA 116970
Digitally signed by EDGARDO RIVERA-URRUTIA 116970
Date: 2020.10.28 16:11:17 -04'00'

Information Security Systems Officer, Edgardo Rivera

Christopher Brown 101386
Digitally signed by Christopher Brown 101386
Date: 2020.10.28 14:43:41 -05'00'

System Owner, Christopher Brown